5 FAM 860
HARDWARE AND SOFTWARE MAINTENANCE

(CT:IM-104;   04-07-2009)
(Office of Origin: IRM/BPC/PRG)

5 FAM 861 CONFIGURATION MANAGEMENT

5 FAM 861.1 Overall Department Policy

(CT:IM-104;   04-07-2009)

a. Configuration management (CM) is the detailed recording and updating of information that describes Department information systems and networks, including all hardware and software components. Configuration management records versions and updates that have been applied to installed software packages and the locations and network addresses of hardware devices. When a system needs a hardware or software upgrade, a system manager can access the configuration management program and database to see what is currently installed. The system manager can then make a more informed decision about the upgrade needed.

b. Configuration management is also used in software development to help developers keep track of the source code, documentation, problems, and changes requested and implemented.

c. Configuration management provides assurance that an information system in the operational/maintenance phase of its lifecycle is the correct configuration and that any changes made are reviewed for security ramifications prior to implementation. Configuration management ensures that changes take place in an identifiable and controlled fashion and have been tested to preclude adverse affects on the information system’s functionality, including its security posture or any connecting Department information system’s security posture.

d. Department information systems must be configured in accordance with the standards established by Information Technology Change Control Board (ITCCB) and/or the Bureau of Diplomatic Security (DS).

e. Network changes that may potentially or directly affect more than a single Local Area Network (LAN) or local network segment must be approved by the IT CCB prior to implementing the changes. Changes that affect only a LAN may be approved by a Local CCB. All documentation recording any network changes approved by the Local CCB must be included in the affected system's security documentation (i.e., Systems Security Plan (SSP), Contingency Plan (CP), etc.). In addition, all documentation recording any network changes must also be forwarded to the IT CCB within 30 days of Local CCB approval.

f. Department configuration management plans must be maintained on all Department information systems. To support this activity, Information Management Officers (IMOs) and Information Security Officers (ISOs) System Administrators will develop and maintain a configuration management plan for the networks under his or her management authority. A configuration management plan will be developed and maintained as part of a system's security documentation for each system required to undergo certification and accreditation (C&A).

5 FAM 861.2 Standard Operating Environments

(CT:IM-104; 04-07-2009)

a. A Standard Operating Environment (SOE) is a specification for using a standard architecture and applications within a Department information system.

b. An SOE supports development of strong configuration management plans for the computing environments commonly used throughout the Department.

c. An SOE is a subset of the overall IT CCB-approved hardware and software baselines approved for Department use. For example, the SOE for desktops or servers.

d. Use of an SOE ensures that the following goals are met:

(1) The components of an SOE will be efficiently and effectively maintained. Only IT CCB approved implementation, configuration, deployment, and upgrade methods are authorized. Regular vote of the IT CCB will insure that the SOE is regularly updated. Communication channels of the IT CCB (meetings, Web site, standard forms, etc) will insure that current and future forms of the SOE are effectively communicated throughout the Department; and

(2) All components of an SOE are expected to have a standard life cycle

which consists of implementation, maintenance, and ultimate disposal and removal from the IT CCB-approved baseline. Only current Department-supported or approved vendor versions of SOE components can exist within the Department.

(3) There are a limited number of versions of any component on an SOE.

(4) New versions of components comprising an SOE must be approved by the IT CCB. A Local CCB does not have approval authority for approving new versions of SOE components.

(5) All SOE components previously approved by the IT CCB must be compatible with new SOE components. Previously IT CCB approved hardware and software that is not compatible with new SOE components must be upgraded or removed according to direction provided by the IT CCB.

(6) The configuration of the SOE must comply with appropriate Department information security and configuration standards. (See 12 FAM 600.)

(7) Any exclusion to this policy will be outlined in the IT CCB Standard Operating Procedure (SOP).

(8) In accordance with 5 FAM 915.14, the IT CCB administers the creation, maintenance, and deactivation of components comprising an SOE. (See the IT CCB SOP.)

5 FAM 862 LOCAL CHANGE CONTROL BOARDS

5 FAM 862.1 Local CCB Responsibilities

(CT:IM-104; 04-07-2009)

a. A post and bureau that maintains systems or applications in support of the Department’s or local mission must establish a Local CCB.

b. A Local CCB is charged to ensure that the hardware, software, or network components installed on a LAN does not adversely affect the existing local IT infrastructure under the operational control of bureau/post IT personnel. The Local CCB must also ensure that all locally approved software and hardware functions only inside the post’s supporting LAN segment.

c. A Local CCB is responsible for maintaining its contact with the IT CCB Voting Representative, as outlined in the IT CCB SOP. When a post/site/bureau Local CCB baseline is established and updated, it must be immediately communicated to the IT CCB voting representative, who in turn communicates the information to the IT CCB.

d. Local CCBs must ensure that the Department's Information Technology Application Baseline (ITAB) includes current, complete, and accurate data on all general support systems, minor and major applications (see 5 FAH-11 H-014), and other IT resources approved for installation on a Department network, or IT resources that contain Department data, including Web sites commissioned on behalf of the Department, bureau, office, division, or post.

e. The Local CCB shall include steps in its process for locally approving commercial off the shelf (COTS) IT resources by:

(1) Reviewing industry sources (to be specified by IA) about vulnerabilities of those IT resources, and making remediation of any vulnerabilities that pose a threat to the network or Departmental data a condition to approval of the software; and

(2) Making a conscious decision whether to request and obtain vulnerability scanning of these IT Resources by DS as a condition for approval. Thereafter, this review and condition process shall be repeated at least annually, supplemented with data on actual configurations from vulnerability and compliance scanning as technically feasible and justified by the level of acceptable risk.

f. The Local CCB shall verify that the local applications' administrators promptly review all vulnerability scanning and configuration compliance data about the locally managed IT resources (provided by IRM, DS, and/or other Departmental security authorities) to identify and remediate vulnerabilities and configuration compliance issues to a level of risk considered acceptable to the Department.

5 FAM 862.2 Local CCB Memberships

(CT:IM-104; 04-07-2009)

a. The Local CCB should consist of a Local CCB chairperson and added members as appropriate.

b. For generic information, see IT CCB Web site.

5 FAM 862.3 Determining What Must Be Sent to the IT CCB

(CT:IM-104; 04-07-2009)

a. If the Local CCB determines that an application would function outside the local network (or LAN) it must obtain IT CCB approval to use the application.

b. All wireless equipment must be approved by the IT CCB. Local CCB approval of wireless equipment is not authorized.

c. All hardware and software used on a classified system must be IT CCB approved.

d. See IT CCB Web site for information on Local CCB, IT CCB requirements, and membership.

e. All updates to the Local CCB must be immediately communicated to the IT CCB voting representative.

5 FAM 863 OPERATING SYSTEM SOFTWARE CHANGE CONTROL

(CT:IM-104; 04-07-2009)

a. Only IT CCB approved Operating Systems may be operated on the Department's enterprise networks.

b. The IT CCB will authorize, at most, two versions of PC operating systems, and two versions of server operating systems for use on the Department's network.

c. System Administrators must notify DS before installing operating systems software that has not been used before in the Department. See 12 FAM 623 and 12 FAM 633. For a list of currently approved operating system software, see the IT CCB Web site.

5 FAM 864 APPLICATION SOFTWARE AND CHANGE CONTROL

(CT:IM-104; 04-07-2009)

a. Application software change controls must be implemented for major and developed applications installed on Department systems:

(1) Define requirements, including security, in the system development and acquisition stage for system confidentiality and availability as well as integrity of data input, transaction processing, and data output;

(2) Initiate the systems authorization process;

(3) Test the application in a development environment, or test bed, prior to operation to ensure the presence of satisfactory operation of controls (this is usually the certification process);

(4) Monitor security controls for vulnerabilities throughout the deployment, operation, and maintenance stages;

(5) Limit access to software programming libraries;

(6) Protect system documentation, as appropriate, with the same due diligence as the data that are protected; and

(7) Operate the IT CCB approved SOE without negative impact to other SOE components.

b. Each System Owner must ensure integrity of major applications and operating system software by implementing documented and effective configuration management procedures, including procedures to:

(1) Restrict the ability to change software (update, upgrade, install, and uninstall) to only those authorized by the system owner;

(2) Audit all changes and maintain a secure copy of the audit;

(3) Maintain a secure copy of changes (old and new software); and

(4) Test all changes on non-live data before deploying changes in a live environment.

c. Each application must be approved either by the Department IT CCB or by the local CCB, as appropriate, before it is used. See 5 FAM 862.3.

d. All Government-off-the-shelf (GOTS) or commercial-off-the-shelf (COTS) applications must be placed into Information Technology Application Baseline (ITAB), and ITAB updated whenever such applications are changed. Posts and bureaus are responsible for providing updates to the ITAB for applications they develop or purchase. See the ITAB Web site for instructions on adding and updating information in the ITAB.

5 FAM 865 COPYRIGHTED SOFTWARE

(CT:IM-104; 04-07-2009)

a. Department employees and contractors may use and distribute commercial software only in accordance with U.S. copyright laws and manufacturer's licensing agreements.

b. The IT Asset Management Branch (IRM/OPS/ENM/NLM/ITA) manages the enterprise software licensing agreements for the Department. (See 5 FAM 915.11-1 e.)

c. The Information Management Officer (IMO)/Information Systems Officer (ISO)/System Administrator must install copyrighted software in conformity to the Department's enterprise licensing agreements, or locally approved licensing agreements.

d. The IMO/ISO/System Administrator must inform IRM/OPS/ENM/NLM/ITA of locally approved licensing agreements or locally funded versions of IT CCB approved software.

5 FAM 866 PATCH MANAGEMENT

(CT:IM-104; 04-07-2009)

a. The purpose of the Department's Enterprise Patch Management Program is to protect data confidentiality, integrity, and availability by mitigating software and hardware vulnerabilities through proactive patch management.

b. The Networks Life-Cycle Management Division (IRM/OPS/ENM/NLM) manages the Department's Enterprise Patch Management Program.

c. IMOs/ISOs/System Administrators must follow guideline and procedures established by the Department's Enterprise Patch Management Program and apply patches in an expeditious manner.

d. The Designated Approval Authority (DAA) may disconnect any system, LAN, or domain that does not comply with the Department's Enterprise Patch Management Program's directives.

e. The Enterprise Patch Management Program will only patch the newest versions of approved Soft Ware (SW) products within its scope.

5 FAM 867 DOCUMENTATION

(CT:IM-104; 04-07-2009)

Documentation of all aspects of computer support and operations is important to ensure continuity and consistency through out the Department of State. Documentation must include:

(1) Current security plans, contingency plans, and risk analyses;

(2) Sufficient documentation to explain how software/hardware is used, including operational procedures;

(3) A current list of workstations (including stand-alones), printers, servers, and other network peripherals/devices (e.g., scanner), the office in which each is located, the cable number/ device number, and port in the hub/switch/router where each is located;

(4) A current list of all the software applications used, the names of the principal users, and the person/office to contact for operational issues or problems;

(5) An annual system performance report;

(6) A systems operations log. This log must be maintained for six months. (See 12 FAM 629.2-11 Log and Record Keeping or 12 FAM 632.5 Log and Record Keeping);

(7) An annual security self-assessment, in accordance with guidance IRM/IA will provide each year;

(8) Audit records on servers and workstations for six (6) consecutive months; and

(9) The current configuration management plan for the bureau/post.

5 FAM 868 THROUGH 869 UNASSIGNED